FireEye
SECURITY REIMAGINED

University of Arizona: You can't fix what you can't see!

SECURITY
REIMAGINED

CUSTOMER SPOTLIGHT

"Oh no! Was it us that was hit?" This was the first question that entered Chris Schreiber's head on reading that Chinese hackers had used a number of compromised US university systems to stage their latest spying campaign.

As the information security officer for the University of Arizona (UA), Schreiber definitely had reason for concern. Being able to definitively determine if a breach has occurred is of paramount importance in knowing what immediate actions to take and how to mitigate against similar threats in the future.

The University of Arizona, ranked in the top 20 U.S. public universities, has more than 40,000 students and over 15,000 employees. With an operating budget of $2 billion, the university collects in excess of $600 million in annual research funding. Renowned for its extensive studies into space exploration, UA receives more NASA grants annually than the next nine NASA-funded universities combined.

Higher education IT systems hold significant volumes of sensitive records, including personally identifiable information, financial data, and R & D related materials. Over the past few years universities have become prized targets for cyber criminals.

The onslaught of attacks on commercial entities has resulted in organizations tightening their cyber defense measures. "As industries like aerospace, biotech, and energy have improved their security, cyber hackers have looked for alternatives," noted Schreiber. "Coming from a traditional mindset of collegiate, collaborative, open thinking has frequently made higher education easy prey for hackers."

THE UNIVERSITY
OF ARIZONA

A recent FireEye Maginot Line report (available via free download on FireEye.com) revealed that 76% of aerospace organizations were breached versus almost 100% of the higher education establishments polled. "The likelihood of a university breach is tremendously high: both with the intent of compromising data, as well as being used as the conduit for other attacks," stated Schreiber.

To place the university in a position to handle the exponentially increasing number and sophistication of cyber threats, Schreiber implemented a layered defense architecture that includes the analysis of data from numerous sources across the infrastructure. "We apply industry-leading threat intelligence, rules, and analytics to the fire hose of data that we generate – such as connection logs, files in transit, web requests, as well as event-related information – and use it to focus on detection and fast response," Schreiber explained.

A long-term FireEye client, the University of Arizona utilizes the cloud-based FireEye Threat Analytics Platform to manage millions of indicators that are updated daily and to perform sub-second searches across billions of events. Schreiber commented, "We're now able to make decisions based on data rather than intuition.

"For example, by monitoring and correlating foreign VPN usage with campus Wi-Fi access, we determined that 63% of all VPN sessions were using stolen credentials. From this we were able to irrefutably justify the implementation of multi-factor authentication, which elevated security across the entire UA environment."

Another example was the highlighting of unusual domain names in the top DNS queries occurring across campuses to identify possibly misconfigured DNS servers that could be used to stage a denial of service attack. By being able to quantify the scope and potential severity of the vulnerabilities, the UA security team was able to justify adding resources to improve the integrity of the network infrastructure.

Schreiber reflected, “We've leveraged a best-of-breed combination of innovative commercial software and open source technologies to enable us to make fully informed, data-driven decisions. It's imperative to get visibility early: You can't fix what you can't see!”

Schreiber was pleased to confirm that even though the attack that originally caught his attention did impact several southern state universities, UA was not one of them.

For more information, please visit: https://www.fireeye.com/solutions/government.html
or send us email at: info_SLED@fireeye.com

Chris Schreiber is the information security officer for the University of Arizona and is responsible for all aspects of information security. He has more than 15 years of experience leading technology and information security teams in higher education and consulting organizations. Chris is a graduate of Central Michigan University and the University of Wisconsin - Madison and holds credentials in information security management, project management, and IT service management.

The University of Arizona utilizes the cloud-based FireEye Threat Analytics Platform and has been a long-term partner and collaborator with the company.